PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-091456
(43)Date of publication of application : 28.03.2003

(51)Int.Cl. G06F 12/14
G06F 17/60

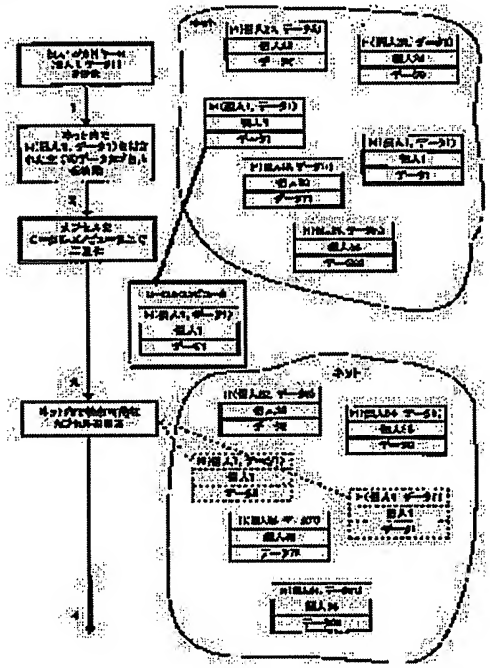
(21)Application number : 2002-156377
(22)Date of filing : 29.05.2002

(71)Applicant : SIEMENS AG
(72)Inventor : KLEINSCHMIT PETER

(30)Priority
Priority number : 2001 10126138 Priority date : 29.05.2001 Priority country : DE

(54) PERSONAL ELECTRONIC HEALTH FILE SYSTEM PROTECTED BY DATA DESTRUCTION OR ILLEGAL READING PREVENTING COUNTERMEASURES

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a personal electronic file system protected by data destruction or illegal reading preventing countermeasures.
SOLUTION: In this electronic health file system protected by safety measures for managing all data associated with the health of a patient including the past medical examinations and treatments in the form of a data capsule on a plurality of distributed servers of a network having an access code permitted by the patient, each time the called data capsule is changed or supplied, the old data capsule in the network is erased, and a new access code is prepared, and the data capsule changed based on the code is newly stored in the network again.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－91456
（P2003－91456A）
(43)公開日　平成15年３月28日(2003.3.28)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード*(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ　５Ｂ０１７
17/60	１２６	17/60	１２６Ａ

審査請求　未請求　請求項の数14　ＯＬ　（全９頁）

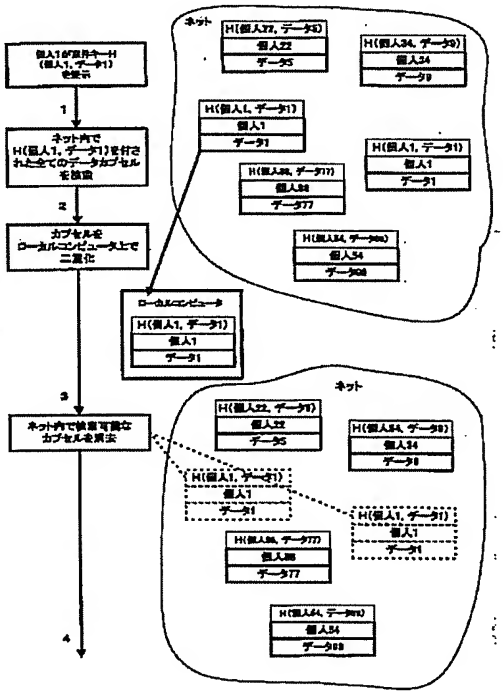
(21)出願番号　特願2002－156377(P2002－156377)
(22)出願日　平成14年５月29日(2002.5.29)
(31)優先権主張番号　１０１２６１３８．１
(32)優先日　平成13年５月29日(2001.5.29)
(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　390039413
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－80333　ミュンヘン　ヴィッテルスバッハープラッツ　２
(72)発明者　ペーター　クラインシュミット
ドイツ連邦共和国　91058　エルランゲン　ゲッペルトシュトラーセ　126
(74)代理人　100075166
弁理士　山口　巖

Ｆターム(参考)　5B017 AA01 BA06 CA16

(54)【発明の名称】　データ破壊や不正閲覧防止策を施された個人的電子健康ファイルシステム

(57)【要約】
【課題】　データ破壊や不正閲覧防止策を施された個人的電子ファイルシステムを提供する。
【解決手段】　過去の診断および治療を含む患者の健康関連の全データを、患者により許可されるアクセスコードを備えたネットの複数の分散したサーバ上のデータカプセルの形で管理するための安全策を施された電子健康ファイルシステムにおいて、呼び出されたデータカプセルを変更もしくは補充する毎に、ネット内の古いデータカプセルが消去され、かつ新規のアクセスコードが作成され、そのコードのもとで変更されたデータカプセルが再び新規にネット内に記憶される。



1

【特許請求の範囲】

【請求項１】　過去の診断および治療を含む患者の健康関連の全データを、患者により許可されるアクセスコードを備えたネットの複数の分散サーバ上のデータカプセルの形で管理するための安全策を施された電子健康ファイルシステムにおいて、呼び出されたデータカプセルの変更または補充毎にネット内の古いデータカプセルが消去され、かつ新規のアクセスコードが作成され、そのコードのもとで変更されたデータカプセルが再び新規にネット内に記憶されることを特徴とする電子健康ファイルシステム。

【請求項２】　アクセスコードがハッシュキーの形式の個人的データおよびメモリデータから作成されていることを特徴とする請求項1記載の健康ファイルシステム。

【請求項３】　アクセスコードが特に安全策を施された変更権限を含み、この権限により古いデータカプセルの自動的消去が行われることを特徴とする請求項１または２記載の健康ファイルシステム。

【請求項４】　データカプセルが不正閲覧防止策を施されたエクストラネット（フリーネット）内に記憶されていることを特徴とする請求項１ないし３の１つに記載の健康ファイルシステム。

【請求項５】　データカプセルが自己組織的に異なったサーバに転送され、多数回同一に記憶され、その際に生じるおそれのある痕跡が失われて遡及不可能となるように、エクストラネットが形成されていることを特徴とする請求項４記載の健康ファイルシステム。

【請求項６】　患者がカウンタのパラメータ化により同一の安全コピーの数を決定できることを特徴とする請求項５記載の健康ファイルシステム。

【請求項７】　データが暗号化されて記憶されていることを特徴とする請求項1ないし６の1つに記載の健康ファイルシステム。

【請求項８】　非対称鍵が使用されることを特徴とする請求項７記載の健康ファイルシステム。

【請求項９】　私的鍵もしくは一対の鍵が、記憶されているデータカプセルの個人的部分の内容を読み取るための個人的権限情報の構成要素であることを特徴とする請求項８記載の健康ファイルシステム。

【請求項１０】　データカプセルの内容が特別なサブアクセスコードによって相応に権限を付与された第三者、たとえば医師、製薬会社などにより限定された範囲で読み取り可能であることを特徴とする請求項１ないし９の１つに記載の健康ファイルシステム。

【請求項１１】　アクセス装置が、データの一定部分を統計学データとして抽出し、補充し、合併し、また図式化することを可能にするようになっていることを特徴とする請求項１０記載の健康ファイルシステム。

【請求項１２】　匿名化された統計学データが、グローバルに通用するカプセルアドレスを備えている特別な統

2

計学カプセルへ入力および記憶されることを特徴とする請求項１１記載の健康ファイルシステム。

【請求項１３】　アクセスコードが特にポータブルアクセス装置（たとえばカード、携帯電話、時計、ブローチなど）に内蔵されており、これらの装置はそれ自体の権限証明システムにより安全策が施されていることを特徴とする請求項１ないし１２の1つに記載の健康ファイルシステム。

【請求項１４】　患者ファイルの少なくとも一部が医師、サービス実行者などの格納装置に記憶されており、これらは患者がアクセスできるようになっており、しかもカプセルアドレスが失われた場合、これらのコピーから新しいデータカプセルが再構成可能であることを特徴とする請求項１ないし１３の１つに記載の健康ファイルシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、過去の診断および治療を含む患者の健康関連の全データを、患者により許可されるアクセスコードを備えた複数の分散したネットサーバ上のデータカプセルの形で管理するためのデータ破壊や不正閲覧に対する安全策を施された電子健康ファイルシステムに関する。

【０００２】

【従来の技術】患者を実際に治療する場合、治療担当医にとっては病歴および患者固有のデータ（接種、アレルギー、配合禁忌など）に関するできるだけ完全なデータを把握することがきわめて重要である。この場合、完全とは必ずしも高度に詳細なことを意味していない。一方、これらのデータは繊細に扱うべきであり、間違った人の手に渡すことは許されない。治療担当医は自分の記憶だけでなく、患者ファイルの形での記録文書を利用し、別の医師へ所見状を送る場合に最重要なデータを所見状に記載する。このことから、実地診療では患者がたまたま時間的理由やその他の理由から同僚医師のデータを入手する方法を持たない新しい医師により受診される場合、問題が生じる。また、これらのデータは患者には限定的にしか利用できないので、ネット上で種々の医療サービスが患者に提供される場合に将来的に技術的および法律的に問題となる可能性もある。

【０００３】これまでもすでに、電子通信手段を用いてこの問題を解決しようとする多くの提案および試験設備が存在している。これらは一方では、個人的に自分で保持すべき患者ファイル（たとえば電子チップカード）に関するか、あるいはまた、各医師がアクセス可能な中央のネットサーバに関するものである。この場合、すでに数年前から議論されいくつかの国では導入されている純粋なカード方式は、第一にデータ量が制限されていること、第二に通信サービスに対するデータの提供が許されていないこと、第三に機械的にしかモバイルコンピュー

タに統合できないこと、またキーボード、バーコードもしくは電子タグによる入力が不可能なことなどの問題がある。

【０００４】上述の集中患者ファイルシステムは、インターネット支持者によって再三再四宣伝されている。この場合、第一に統一的なデータ規準がないのでこの種の患者ファイルシステムは実地には実施不可能であるという難点が生じる。さらに、データ利用に関する法律的問題、最終的には保証できない安全性に関する処置に費用がかかること、その結果データの破壊工作および不正使用によるデータ喪失のリスクが生じる。インターネットにおけるプロバイダですでに実験的に導入されている私的ファイルの作成も、この問題を解決できない。というのは、管理不可能なデータの転送が危惧され、データのプライバシーが保障されず、データも多くの場合互換性を持たないからである。

【０００５】この安全性の欠如は、冒頭に挙げた種類の健康ファイルシステム、すなわち健康関連データが、たとえば国際特許出願公表第０１／１８６３１Ａ１号に提案されているような、患者により許可されるアクセスコードを備えた、ネットの複数の分散したサーバ上のデータカプセルの形で記憶されている健康ファイルシステムに対しても該当する。アクセスコードがたった1回でも間違った人の手に渡った場合は、国際特許出願公表第０１／１８６３１Ａ１号によるこのような比較的安全なシステムでもデータの絶え間ない不正使用は阻止不可能である。

【０００６】

【発明が解決しようとする課題】したがって本発明の課題は、データ破壊工作や不正閲覧に対する安全策を施されており、また、データの無権限な転送もしくは無権限な利用に対する高い安全性を有する確実な電子健康ファイルシステムを提供することにある。

【０００７】

【課題を解決するための手段】本発明によれば、この課題は、呼び出されたデータカプセルを変更もしくは補充する毎に、ネット内の古いデータカプセルが消去され、新規のアクセスコードが作成され、このコードのもとで、変更されたデータカプセルが再び新規にネット内に記憶されるようにすることにより解決される。

【０００８】データカプセルの変更もしくは補充の際にこのようにアクセスコードを自動的に変更しても、何らかの方法でたとえばあるデータを1回だけ閲覧する権限を有していったんアクセスコードを入手した無権限者は、データカプセルが変更されていない限りはこれらのデータを繰り返し閲覧することが可能である。しかしデータカプセルの変更毎にアクセスコードの変更も必然的に行われ、この新規のアクセスコードのもとで変更されたデータカプセルが記憶され、同時に古いデータカプセルの消去が行われる。したがって、古いアクセスコードを所有している無権限者にとってはこれらの古いデータへのアクセスもほとんど不可能となる。というのは、これらの古いデータはデータカプセルがいったん変更された場合はすべて消去されるからである。

【０００９】本発明の実施態様によれば、ハッシュキーのような個人的データおよびメモリデータから作成されているアクセスコードは、特別な安全策を施された変更権限を含み、これを通じて古いデータカプセルの自動的消去が行われる。これによって、有資格権限者が、アクセスコードに変更権限が含まれていない第三者にサブアクセス権限を与え、その結果この第三者がデータカプセルを呼び出したり、閲覧することはできるが、変更することはできないということになる。

【００１０】この場合、別の実施態様によれば、各アクセスを時間記録しているログファイルを通じてデータカプセルからデータを閲覧することも変更を意味し、この変更がアクセスコードの自動的変更をもたらすようにされる。しかし、これは有権限者で同時に変更権限を有する者によりデータの閲覧が行われる場合にのみ有効である。というのは、そうでなければ第三者によるデータ閲覧を許した場合、古いデータカプセルが消去され、変更されたアクセスコードを備えた新規のデータカプセルが記憶されてしまうので、本来の所有者にもこれらのデータカプセルの検索が不可能となってしまうからである。

【００１１】データカプセルの消去および後続の新規書き込みは、いわゆるフリーネットのリソースをさらに活用することをもたらし、フリーネットに格納されているデータカプセルの冗長性を増す。というのは、かなりの長期間にわたれば、数人の関係者がこのネットから離脱し、その場合、データカプセルの1つもしくは複数のコピーが失われるという危険がフリーネットには存在するからである。

【００１２】この場合、データは、ここで言われているデータカプセル（場合によっては異なったアクセスコードを備えている）の形でメモリネットワークに記憶されるのが望ましく、このメモリネットワークはインターネットのような広範に利用可能なネットワークであり、このネットワークには場合によってはデータを記憶するためのフリーネットなどの不正閲覧防止策を施されたエクストラネットが形成される。このフリーネットはインターネットで保証付きソフトウェアにより誰にでも利用可能であり、この場合、この保証付きソフトウェアは、上記の機能のほかにデータへの不法なアクセスを可能にするような裏口を持っていないことを保証している。

【００１３】この場合、インターネット内の上述のエクストラネットは、データカプセルが自己組織的に異なったサーバへ転送され、何度も同一のものとして格納され、その際に生じるおそれのある痕跡が失われ、遡及不可能となるように作成されている。

【００１４】さらに、このような多数回の格納は、この

場合患者がカウンタのパラメータ化により同一の安全コピーの数を決定できるので、電子健康ファイルの匿名化されたデータカプセルの１つを保有するメモリがたまたま破損してもこれらのデータが喪失されないという利点がある。というのは、多数の安全コピーはメモリネットへ多数回配分された後でも同じサーバ上に格納されていないからである。

【００１５】この種のデータカプセルは、いずれにしても患者だけが所有し、患者が医師、サービス実行者、健康保険組合などの第三者にごく例外的に、またおそらくは限定された範囲内でのみ使用させるような、任意に複雑化して作成可能なアクセスコードを用いてのみ読み取り可能であるが、このこととは無関係に、追加的な安全保障としてさらに、データを暗号化して記憶するようになっている。この場合カプセルの暗号化には特に非対称鍵が用いられ、同時に、患者ファイルの暗号化用の患者の公的鍵ならびに復号化用の患者の私的鍵も用いられ、また、この私的鍵もしくは一対の鍵は個人的な権限情報、すなわちデータカプセルの内容を読み取るための個人的アクセスコードの別の構成要素でもある。

【００１６】本発明の別の特徴によれば、データカプセルの内容は、相応の権限を与えられた第三者（たとえば医師、サービス実行者、製薬会社、健康保険組合など）の特別なサブアクセスコードによって限定された範囲内で読み取り可能になっており、このために特にデータの一定部分を統計学データとして抽出し、補充し、合併し、図式化することを可能にするアクセス装置が用いられている。

【００１７】この場合、匿名化された統計学データは別の利用のために、特に、権限を付与する患者に一定の利益もしくは報酬を提供する製薬会社もしくは健康保険組合による呼び出しのために、患者の指示に基づいて特別な統計学カプセル（これらのカプセルにはグローバルに通用するカプセルアドレスが備えられている）へ入力および記憶される。したがってこれらの統計学機能を満たすために、患者の個人的健康ファイルの全データに対する本来のアクセスコードの付与は必要ない。

【００１８】この場合、本発明の別の特徴によれば、１つもしくは複数のアクセスコードは特別なポータブルアクセス装置（たとえばチップカード、携帯電話、時計、ブローチなど）へ内蔵することができ、また、公的なアクセス対象物（たとえばネットポータルなど）へも入力可能である。この場合、アクセス装置はそれ自体公知の方法でアクセス装置が失われた場合に不正使用を防止するための認証システム（ＰＩＮ番号など）により確実に安全性が保証されている。

【００１９】また本発明の別の実施態様によれば、カプセルアドレスが失われた場合における完全なデータ喪失を回避するために、医師、ザービス実行者などの側の格納装置内に患者ファイルの少なくとも一部だけが場合によってはこれらの人々が部分的にでも読み取り可能なように記憶されているようになっており、これらの人々は、カプセルアドレスが喪失した場合にこれらのコピーから新しいデータカプセルを再生するために患者にアクセスできる。

【００２０】本発明によるデータ破壊や不正閲覧防止策を施された個人的電子健康ファイルシステムに安全でかつ多種多様な健康利用のために呼び出しできるように記憶されるべき重要な健康情報は、第一に患者の利益のために秘匿すべき長期的情報、すなわち将来的にそのつどの診断もしくは治療にとって重要とみなされるような過去から現在までのデータならびに推測や助言のすべてを含む。これには病歴、所見、最終診断報告、医学的病期の証拠資料（写真、診断画像、ビデオおよび音声記録など）も含まれる。推定診断、中間段階、誤診、否定的所見等々はこれらの成果および将来の予測的意義においてのみ記録すべきであり、詳細に記録する必要はない。この場合、これらのデータの一部を個人的な資料情報の追加として直接個人的なアクセス装置へ入力しておく（たとえば救急データとして）および／もしくは指標すなわち特別なアドレスとして作成しておけば、この指標を通じてバリヤーなしに直接的に本発明による健康ファイルシステムを実現する広範に利用可能なネットワーク（これは現時点ではインターネット）を通じてこれらのデータにアクセスできる。

【００２１】他方では、数時間後に評価されるか処理済みとなり、消去される治療データ、処方、測定値、観察ファイル、助言などの短期的な秘密データがある。これらのデータは相応の間隔で長期的データのストックに追加される。この場合、すでに提案してきたように、短期的および長期的データ用に種々のハッシュアドレスを備えた様々なカプセルが用いられる。これらのハッシュアドレスは同一の個人的なアクセス装置もしくは互いに分離された様々なアクセス装置によっても得ることができる。この選択は前者の場合は操作ソフトウェアもしくは個々のアクセス装置上のコンフィグレーションによって行われる。

【００２２】したがって以上を要約すると、本発明による電子健康ファイルシステムの特徴はデータ構造にあるので、データはネット利用者が患者に対して読み取りの権限を有しているような範囲内でのみ読み取られる。患者自身も、ショックを受けるようなデータから精神的に保護されることを放棄する限り、ファイルの全部を読み取ることができ、患者が書き込み可能な、すなわちデータを変更する範囲を有することもできる。公知のプロフェッショナルカードは、医師に対してもやはり一定の部分にしかアクセスを許可しない。ただし、二重の（多重の）暗号化によって医師には読み取り不可能な部分（いわゆるロールコンセプト）が残る。患者は複数のカプセルを定義し、何に対し、また誰に対してアクセスを認め

るかを決定することもできる。このロールコンセプトは鍵もしくはその他のアクセス制限手段を通じて実現される。

【００２３】

【発明の実施の形態】本発明の利点および特徴の詳細を複数の実施例および図面に基づき説明する。

【００２４】図１には、フローチャートに基づき、まずどのようにして個人１が個人的なデータおよびメモリデータ（データ１と呼ぶ）から作成された案件アクセスコード（キーH）を提示するかが示されている。このキーを用いて、同様のキーによってネットワーク内に記憶されているすべてのデータカプセルが検索可能である。当該のデータカプセル（ここでデータカプセルとは、共通のアクセスコードにより安全策を施された、そのつどのメモリネットワークの要求に従う特別なデータ構造における多数の患者データを意味する）が検索されると、ローカルコンピュータ上でこのデータカプセルのコピーが作成され、案件キーの一部でありかつこのキーで読み取り不可能な変更権限が存在する場合は、ネットワーク内で検索可能な相応のすべてのデータカプセルが消去される。このようなデータカプセルの消去は、図１の右下にネットワーク内にある２つのデータカプセルコピーを点線で囲うことにより示されている。

【００２５】図２は、どのようにして新しい検査結果もしくは新しい時間記録の付加によるデータ１の変更によりデータ２への変更と同時にアクセスコードの変更が自動的に行われるのかを示している。この変更されたアクセスコードによって、ローカルコンピュータ上にある変更されたデータカプセルは従来技術により再び記憶され、ネットワーク内に分配される。これは図２の右下に、２つの変更後データカプセルがアクセスコードH（患者１，データ２）によって記憶されるのが認められる。一方、アクセスコードH（患者１，データ１）を有する古いデータカプセルは依然として消去される。

【００２６】図３はデータ破壊や不正閲覧防止策を施された健康ファイルシステムの構成を図解して示しており、このシステムは患者を自分がアクセス可能なデータの所有者にし、この場合、健康ファイルはインターネットにおける１つもしくは複数の分散型でインデックスフリーのカプセルを含む。

【００２７】図４および図５には、インターネット内に記憶されている健康ファイルへのもしくは健康ファイルからの、ある時は患者自身のために、またある時は医師により許可されている利用者の実施例として記憶および読み取りの種々の方法が示されている。この場合、識別およびハッシュアドレスは原理的には様々な種類のアクセス装置、例えば携帯電話、時計、ブローチ、トランスポンダの形の電子ラベルに、バーコード読み取り器もしくはキーボードによるコード入力などにより配置される。図示されている実施例ではこれはチップカードにより実現されており、このチップカードはその構成およびデータ構造が詳細に図解されている。

【００２８】たとえば図５によれば本発明による個人的な電子健康ファイルシステムは医師により以下のように利用可能である。実体的に存在する患者は医師に物理的な個人的患者ファイルを渡し、医師はインターネット内のカプセルを見つけ出し、そのカプセルを患者カード（および医師カード）によって開封する。医師は治療事実および治療予定日を記入し、ローカルコピーを作り、（たとえば医師にとって既知もしくは未知の）新規の最終ハッシュアドレスによって再びカプセルを閉鎖し、この新規カプセルを再びインターネット内へ格納する。この場合ハッシュアドレスが変更されると、すべての古いカプセルは相応に予定されているプログラム部分を実行することにより消去される。医師はその後は重要な中間診断まで自分のローカルコピーで作業し、このコピーを所見状の作成および通信医療サービス用に使用する。患者はネット内の認証により自己証明することができる。治療結果の患者カードへの追加記入は分離して行う必要がある。非対称鍵の場合は、医師に有効なハッシュアドレスが告げられるかこれが変更されていなければ、患者カードがなくても記入可能である。

【００２９】図６には健康ファイルの検索や意義の種類による健康ファイルの種々の文書形式が示されており、異なった等級の暗号化方法および異なったアクセス方法が示唆されている。特に、カプセルＢに記憶されている患者データ（この場合も当然のことながら複数の異なったデータカプセルである）は、秘密保持の必要はなく、かつたとえばいわゆる統計学データ（相応のサービス実行者によって患者への相応の報酬と引き換えにいつでも呼び出し可能である）に属するデータに相当する。

【００３０】治療、所見状もしくは処方せんの作成の場合にインターネット内の個人的電子健康ファイルへのアクセスカードとしてチップカードを用いる方法は図７にフローチャートとして示されている。一方、すでに述べたように図８は、電子記憶されている健康カードへの患者の個人的アクセスカードとしてのチップカードについて種々のアクセス方法を詳細に説明している。

【００３１】通信医療用の個人的健康ファイルを使用するには、医師はたとえば自分のローカルコピーからのデータおよび医師が所望する技術を用いて作業し、これらのデータを通信サービス用に使用する。患者はインターネット内の自分の認証を用いて自己証明することができ、したがって権限を有する者として通信医療サービスに参加することができる。

【００３２】個人的患者ファイルは、そこへデータの書き込みが可能で、そこからデータの読み取りが可能な別の範囲を有することもできる。この場合、これらの範囲はハッシュアドレス作成用に空けてあるので、これらの範囲へのデータ書き込みはハッシュアドレスの変更をも

たらさない。これらの範囲は私的な健康管理のためにも利用可能であるので、各種装置からの測定値およびおよび薬剤のラベルのデータ並びに補助的な治療手段がここに書き込まれる。

【図面の簡単な説明】

【図1】フリーネットに記憶されているデータカプセル上の有権限者のアクセスならびにフリーネットの古いデータカプセルの消去に関するフローチャート。

【図2】ローカルコンピュータ上に配置されているデータカプセルおよびアクセスコードの変更およびネットにおける変更後アクセスコードによる新規記憶のデータ変更に関するフローチャート。

【図3】本発明による安全策を施されたインターネットにおける個人的健康ファイルシステムの解説図。

＊【図4】患者による私的処理のための個人的健康ファイルシステムの解説図。

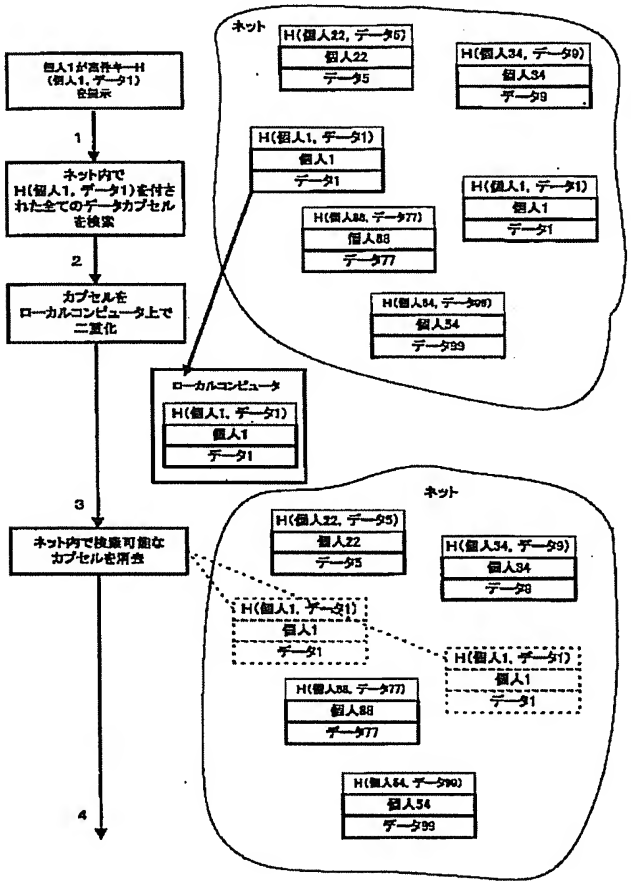
【図5】医師による個人的健康ファイルの処理方法の図４に相応する解説図。

【図6】様々なハッシュアドレスを備えた種々のカプセルへ情報を分配するための健康ファイルの文書形式の解説図。

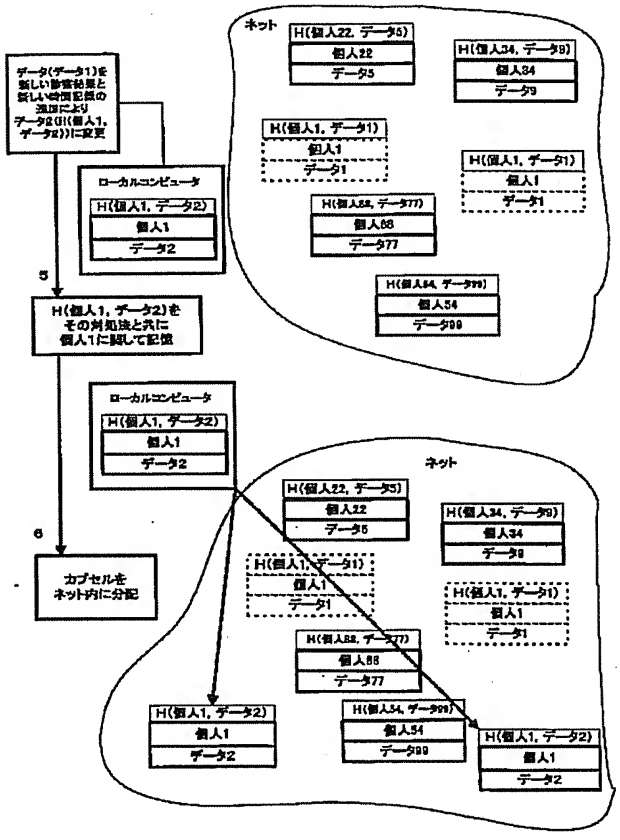
【図7】本発明による安全策を施された健康ファイルの使用下でのインターネットにおけるカードおよび患者ファイルによる治療、所見状および処方せん作成のための解説図。

【図8】インターネットに基づく本発明による健康ファイルへの個人的なアクセスカードの構成図。

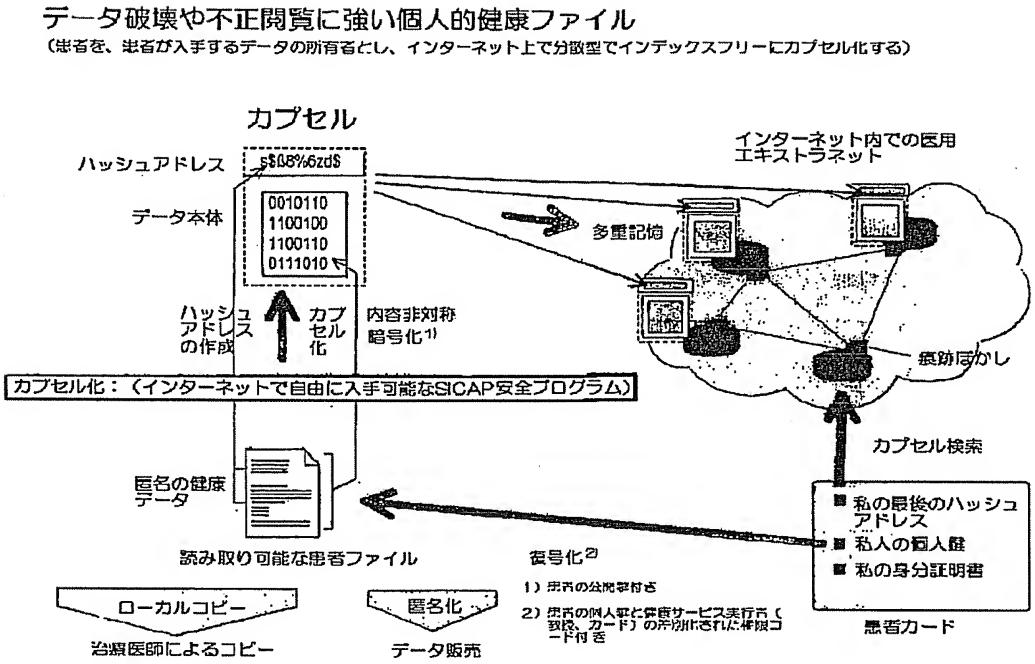
【図１】



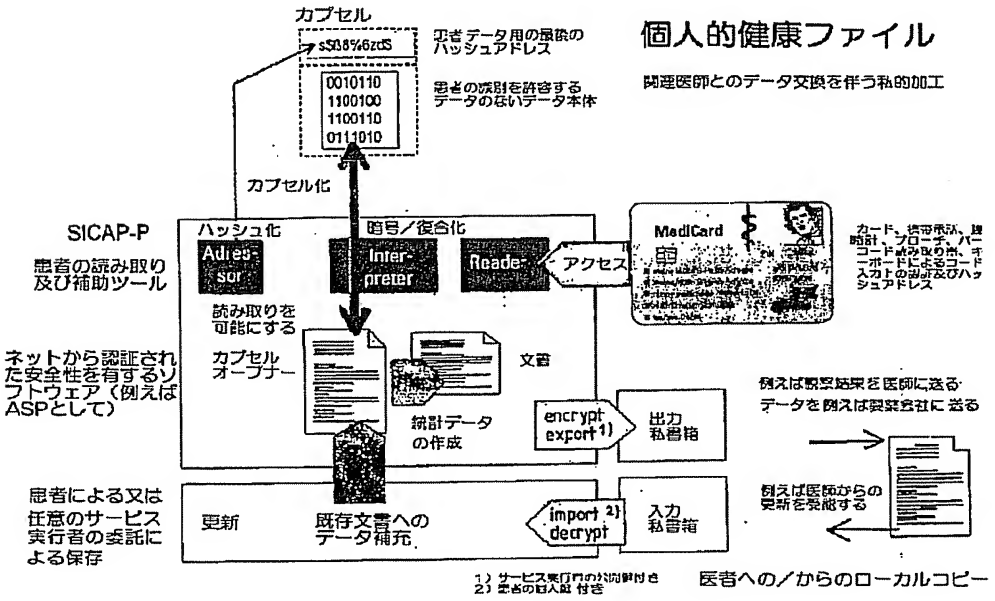
【図２】



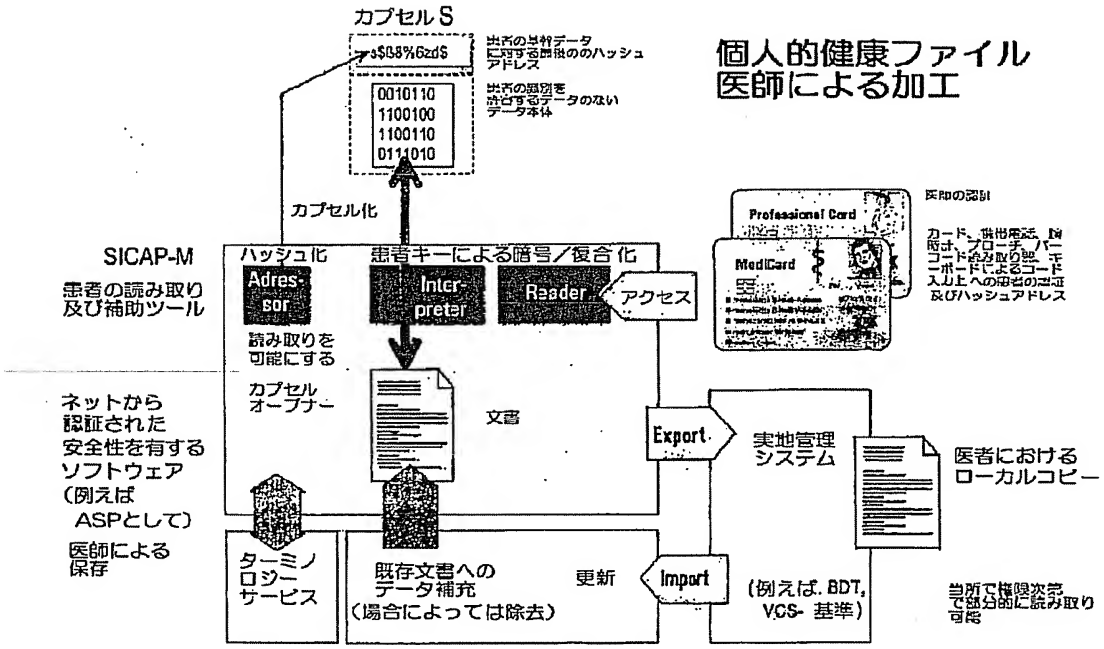
【図３】


データ破壊や不正閲覧に強い個人的健康ファイル
（患者を、患者が入手するデータの所有者とし、インターネット上で分散型でインデックスフリーにカプセル化する）
カプセル
ハッシュアドレス
s$08%6zd$
データ本体
0010110
1100100
1100110
0111010
ハッシュアドレスの作成
カプセル化
内容非対称暗号化1)
インターネット内での医用エキストラネット
多重記憶
痕跡ぼかし
カプセル化：（インターネットで自由に入手可能なSICAP安全プログラム）
匿名の健康データ
読み取り可能な患者ファイル
復号化2)
カプセル検索
私の最後のハッシュアドレス
私人の個人鍵
私の身分証明書
患者カード
1）患者の公開署名付き
2）患者の個人鍵と健康サービス実行者（医師、カード）の承認された権限コード付き
ローカルコピー
治療医師によるコピー
匿名化
データ販売

【図４】


カプセル
s$08%6zd$
患者データ用の最後のハッシュアドレス
0010110
1100100
1100110
0111010
患者の識別を許容するデータのないデータ本体
個人的健康ファイル
関連医師とのデータ交換を伴う私的加工
カプセル化
SICAP-P
患者の読み取り及び補助ツール
ハッシュ化
暗号／復合化
Addres-sor
Inter-preter
Reade-
アクセス
MediCard
カード、携帯電話、腕時計、プローブ、バーコード読み取り機、キーボードによるコード入力のための及びハッシュアドレス
読み取りを可能にする
カプセルオープナー
ネットから認証された安全性を有するソフトウェア（例えばASPとして）
文書
統計データの作成
encrypt export1)
出力私書箱
例えば要求結果を医師に送る
データを例えば保険会社に送る
患者による又は任意のサービス実行者の委託による保存
更新
既存文書へのデータ補充
import 2) decrypt
入力私書箱
例えば医師からの更新を発起する
1）サービス実行者の公開鍵付き
2）患者の個人鍵付き
医者への／からのローカルコピー

【図５】



【図６】

健康ファイルの文書形式

❶ 暗号化せずにすべての人に読み取り可能なデータ（救急時用）

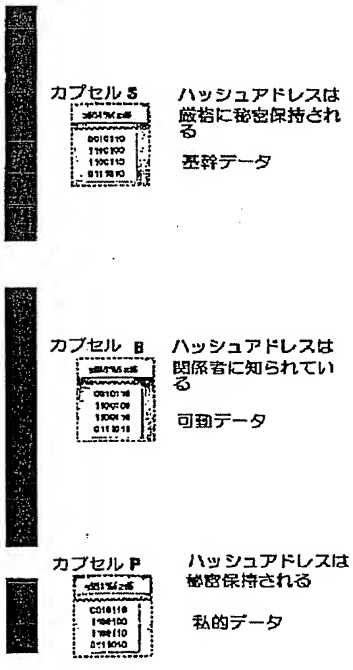
❷ サービス実行者が補充しかつ読み書き可能であり当人（所有者）は読み取り可能な長期間有効なサービスデータ（例えば病歴、投薬、配合禁忌、診断書、写真などの患者ファイルデータ）。読み取り権限は役割により調整される。パラメータ化は認証特徴を介して行われる。所有者は自分がその内容を知ることを放棄したものを除きすべてのデータを読むことができる。

❸ サービス実行者から他の予め知られていない例えば患者により指示すべき別のサービス実行者に伝えられこの実行者が読み書き可能で当人は読み取りのみ可能なダイナミックサービスデータ（例えば未知の人への処方せん、所見状、診断書）

❹ 患者から当初は未知の一人又は複数のサービス実行者に提供させるダイナミックサービスデータ（例えばモニタデータ、質問状）

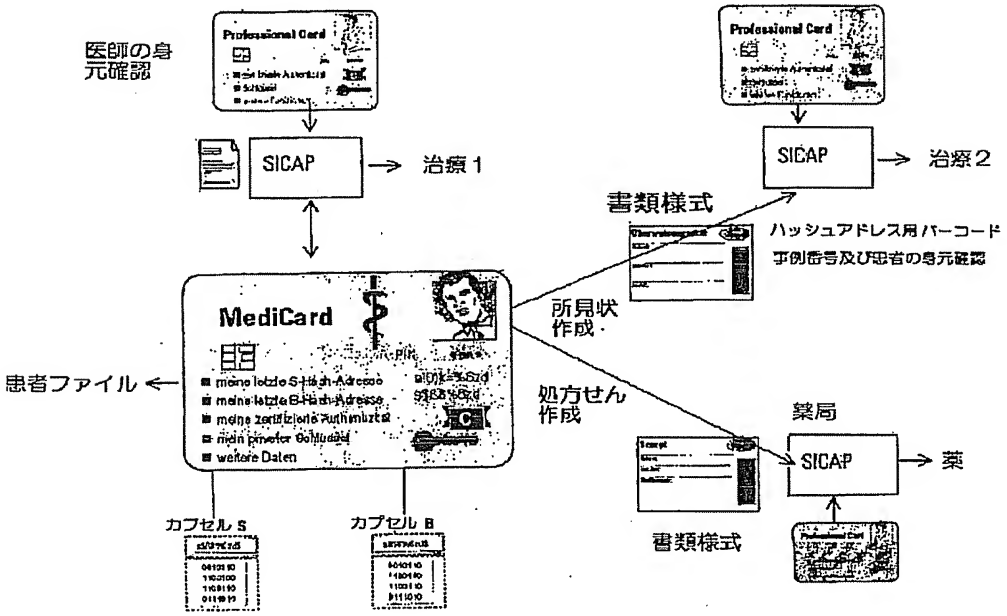
❺ 代理処分：委任状、受能権限……

❻ 所有者のみがアクセス可能な個人的暗号化データ（コンピュータで読み取り可能な任意の文書用金庫）



【図７】

カード及びインターネット上の患者ファイルによる治療、所見、及び処方せんの作成



【図８】

インターネット上の健康ファイルへの個人的アクセスカード